stored in another location in cach software product, and each of thosc another locations is different in different software products so that it would not be discovered and altcred. And, each such softwarc product, when executed, will automatically check thc unencrypted identity storcd therein against the decryption result of the encryptcd one, if they are not consistent, the software product will fail to operate. The idcntity or encrypted identity of the rightful user being included into each of the software products by the central computer at the time when the central computer is to supply the same to thc user computer. Further, to prevent thc AS sub-program from mistakenly regarding a software product which stored in thc computer and which being not supplied from the central computer, as a software product under its control, thc central computer may further include information in a third predetermined location of cach software product for indicating this fact, that is, the software product bcing supplied from the central computer, to the AS sub-program and each software product will not opcratc if when being executed, it finds that information thcrcin bcing altered.

It should bc noted that the above embodiments are given by way of example only, and it will be obvious to those skilled in the art that various changes and modifications may bc made without departing from the spirit of the present invcntion.

What is claimed is :

1.(Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Authorising software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said authorising software being for, when executed, 1) permitting use of said software desired to be protected on said computer ; 2)]

determining [the existence of] if identity [software in a memory] means/information, is existing in a processing device [under control of said computer] ;

using a favourable result of said determination as a pre-condition for said processing device providing user access to said software desired to be protected ;

wherein said identity [software] means/information

[being for use on said computer to provide information of said rightful or authorised user ; said information]

being essentially used [in] by a control means of said processing device for enabling operation(s) for which [said] rightful [or authorised user] user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

[and the existence of said identity software in a memory means under control of said computer is being determined without a said operation being performed by said remote computer]

[wherein use of said software desired to be protected on said computer will not be permitted if said identity software is determined as being not existing in a memory means under control of said computer .]

2. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

[Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1, wherein further comprising software, when being executed, for]

authenticating said identity [software] means/information ;

[and if the result of the authentication of said identity software is unfavourable,]

said identity [software] means/information will [further] be determined as existing [not existing in a memory means under control of said computer], if the result of said authentication is favourable and as not existing if otherwise .

3. (First time Amended) A method for protecting software from unauthorised use ,

[Authorising software, stored in a device or existing physically on a medium,]

as claimed in claim [1] 12, wherein said software desired to be protected being a first software used on said processing device for determining third information related to hardware and/or software of said processing device ;

wherein further comprising [authenticating] second software for , when being executed, authenticating the computer on which [it] said second software runs as being [a particular predetermined computer] said processing device, basing on at least a part of said third information;

[and if the authentication result of the computer on which it runs is unfavourable, said authorising software will not permit use of said software desired to be protected and will permit use of said software desired to be protected]

and access to a third software will be provided if said authentication result [of the computer] is favourable ;

wherein said third software being distributed through a communication network to said rightful user.

[and said identity software is determined as existing in a memory means under control of the computer on which said authorising software runs].

4. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1,]
wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s).

5. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1,]
wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

6. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 5,
[Authorising software, stored in a device or existing physically on a medium, as claimed in claim 5,]
wherein [further comprising] said processing device having an encrypted identity of its rightful user ; and if one of said protected programs stored in said computer has a valid user identity which being not consistent with the decryption result of said encrypted identity [in] of said [authorising software] processing device,

[said authorising software will not permit] use of said protected programs will not be permitted and will be permitted if otherwise .

7. (Second time Amended) Protection software for use on a [computer] processing device, to protect [purchased computer] software publicly distributed by a system against unauthorised use [by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof] ;

said protection software comprising :

identity software [for use on said computer to provide information of said rightful or authorised user ;]

[said information being esentially] essentially used on said processing device in enabling operation(s) for which [said] rightful [or authorised user] user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of the user thereof for, when executed, [permitting use of] providing user access to said software desired to be protected [, on said computer] ;

wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually; and

wherein the improvement resides in said protection depends on no hardware specific to said user(s) .

8. (First time Amended) Protection software [, stored in a device or existing physically on a medium,] as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s) .

9. (First time Amended) Protection software [, stored in a device or existing physically on a medium,] as claimed in claim 7, wherein said authorising software [includes] contains said identity software.

10. (Second time Amended) Authorising program/means [for use on a computer] used in a processing device, to protect other [computer] software against unauthorised use ; [by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof] ;

said authorising program/means being effectively under the control of the user thereof for, [when executed,] providing access to [permitting use of] said software desired to be protected [on said computer] ;

wherein information [of] related to [said] rightful [or authorised user] user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said information being capable of being used essentially, but not in a form to be so used , [used] by said processing device in enabling operation(s) for which said rightful [or authorised user] user(s) has to be responsible .

11. (First time Amended) Authorising program/means [, stored in a device or existing physically on a medium,] as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s).

12. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Protection software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said protection software comprising :]

obtaining a first information from a user of a processing device having an identity software/means ;

using said first information received being correct as a pre-condition for said processing device providing user access to said software desired to be protected;

wherein said identity software/means being for [, with password protection against used by unauthorised user,] providing a second information [of said] related to rightful [or authorised user] user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being essentially used by said processing device in enabling operation(s) for which said rightful [or authorised user] user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

[authorising software for, when executed, permitting use of said software desired to be protected on said computer ;]

[wherein use of said software desired to be protected will not be permitted if a correct password not entered by user .]

13. (First time Amended) A method for protecting software from unauthorised use , [Authorising program , stored in a device or existing physically on a medium,] as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s) and said first information being a password.

14. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Authorising software for use on a computer to protect other computer software by discouraging a rightful or authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said authorising software being for, when executed, 1) permitting use of said software desired to be protected on said computer ; 2)]

authenticating identity [software] information/means [existing in a memory means under control of said computer] associated with a control means of a processing device ;

using a favourable result of said authentication as a pre-condition for said control means providing user access to said software desired to be protected ;

wherein said identity [software being for use on said computer to provide information of said rightful or authorised user ;]

[said] information/means being essentially used by said control means for [in] enabling operation(s) for which [said] rightful [or authorised user] user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

[wherein use of said software desired to be protected will not be permitted if the result of said authentication of said identity software is not favourable .]

15. (First time Amended) A method for protecting software from unauthorised use , [Authorising program , stored in a device or existing physically on a medium,] as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s).

16. (First time Amended) A method for protecting software distributed by a system from unauthorised use , comprising the steps of :

a) obtaining by a processing means of said system, confidential information of rightful user(s) of said software desired to be protected ;

b) creating by said processing means, a first software with said confidential information therein ;

c) transferring ~~by~~ from said system, said first software to a processing device under control of said rightful user(s) ;

d) thereafter, obtaining by said first software running on said processing device , first information from the user thereof ;

e) determining by said first software, from said processing device second information related to the hardware or/and software thereof for future reference in step f) below, in response to said first information obtained being consistent with said confidential information therein ;

f) thereafter, authenticating by a second software, the processing device onwhich said second software is being used, basing on at least a part of said second information ;

h) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

wherein said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; ~~and use of said software desired to be~~ and said steps d) to h) is being performed without causing a said Transaction take place.

[Protection software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;

said protection software comprising :

identity software for, with protection against used by unauthorised user, providing information of said rightful or authorised user ;

said information being in enabling operation(s) for which said rightful or authorised user has to be responsible ;

authorising software for, when executed, permitting use of said software desired to be protected on said computer ;

wherein use of said software desired to be protected will not be permitted if said protected identity software is not being caused to be usable by correct information obtained from user .]

17. A method for protecting software distributed by a system from unauthorised use, as claimed by claim 16, wherein "said first information obtained being consistent with said confidential information" being the only condition for performing said step e).

Said determination in

18. A method for protecting software from unauthorised use, comprising the steps of :

a) transferring from ~~said~~ a software distribution system, said software desired to be protected to a processing device under control of a user ;

b) transferring ~~by~~ from said software distribution system, a first and second software to said processing device ;

c) determining by said first software running on said processing device, say first processing device, if identity information/means which being essentially used by a control means of said processing device for accessing in a remote electronic transaction system an account of said user, is present in said processing device ;

d) establishing a communication between said first software and a control means of said remote electronic transaction system, for verifying said account is a valid account, by said control means of said remote electronic transaction system to said first software ;

e) using by said first software, favourable results of said determination of presence and verification as pre-conditions for determining from said processing device information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said user by said software distribution system, for the first time said steps a) to e) being carried out ; thereafter

f) authenticating by said ~~a~~ second software, the processing device onwhich said second software is being used, say, second processing device, basing on at least a part of said information related to said hardware or/and software ;

g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing device, with no charge ;

if the result of said determination of consistence is not favourable, repeat at least said steps c) to g) with said second processing device, without re-charging from said user said cost ;

wherein said first and second software being specific to said user.

19. A method for protecting software distributed by a system from unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to g) .

omit

20. A method for protecting software distributed by a system through a communication network, from unauthorised use, comprising the steps of :

a) creating by said system, a first software ;

wherein "the presence of identity information/means which being essentially used ~~in~~ by a control means of a processing device for enabling operation(s) for which a rightful user of said software desired to be protected has to be responsible, in said processing device" ; is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

P cont

b) transferring from said system, said first software to said ~~a~~ processing device ~~under control of said rightful user~~ ;

E' amt

c) determining by said first software running on said ~~proceesing~~ processing device meeting said precondition, first information related to the hardware or/and software of said processing device , for future reference in step e) below ;

d) thereafter, determining by a second software, from the processing device onwhich said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

repeat at least said steps c) to f) if said result of said determination of consistence is not favourable, without causing any operation(s) for which said rightful user has to be responsible, being performed ;

wherein said first and second software being specific to said rightful user.

Gp 2132
Copy

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant and Inventor	Ho Keung, TSE.
Title	Software for restricting other software to be used by the rightful user only and method therefor.
Filing Date	07/09/98
Application Number	09/112,276
Group Art Unit	2132
Examiner	Gilberto Barron Jr.
Postal Address	P.O. Box 54670, North Point Post Office, Hong Kong.
H.K. Tel & FAX	(852) 8105, 1090 (852) 8105, 1091
Email	TSE@pat-rights.com

By Airmail & Fax

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Sir,

Formal Amendment Dated April, 02, 2001(20 claims presented)

Pls change the title to read as "Protection of software from unauthorised use".

Regarding the Office action, P.3, section 7, the missing figures 1,2 are the same as those of the parent application.

Pls amend sheet 11 by using the replacement sheet submitted herewith. In the replacement sheet 11, the last paragraph "It should be noted … the present invention." is newly inserted and the first paragraph is originally filed.

In the originally filed specification, P.1, "Field of the Invention", line 1, pls delete "commercial", line 2, pls delete "such".

In the original filed specification, P.2, "Summary of the Invention", second paragraph, last line, pls insert "which may be purchased commercial computer software" after "products". This is no new matter and is consistent with original filed claim 7, line 3.

In the original filed specification, P.5, line 6, pls change "use" to "user".

Respectfully submitted,

Ho Keung, Tse.

COMMENT

All claims being amended. Claims 17-20 are new. 20 clams are presented, in which claims 1, 7, 10, 12, 14, 16, 18, 20 are independent.

Claims 2, 4-6 depends directly or indirectly on independent claim 1.

Claims 8, 9 depend on independent claim 7.

Claim 11 depends on independent claim 10.

Claims 3, 13 depends on independent claim 12. Note that claim 3 originally depends on claim 1.

Claim 15 depends on independent claim 14.

New claim 17 depends on independent claim 16.

New claim 19 depends on independent new claim 18.

The present invention as defined by the independent claims as amended is directed to protecting software from unauthorised use by means of a "psychological barrier". This is an innovative feature of the present invention not being suggested or disclosed by the cited prior art reference, either considered individually or in combination.

Independent claims 1, 7, 10, 12, 14 as amended require existence of identity means(claims 1, 12, 14)/information(claims 1, 10, 14)/software(claims 7, 12) for "operation(s) for which rightful user(s) of the software desired to be protected has to be responsible", as a "psychological barrier".

Regarding the First Office action, P.5, section 13, as the Examiner recognised in the second and third paragraphs therein, that Wiedemer (4,796,181) is directed to a billing system for computer software and the security module 16 contains information therein for enabling billing operation .. take place whenever the protected software is to be executed.

As readable on the amended independent claims 1, 12, 14, their identity means/software/information is for enabling operation(s) for which rightful user(s) of the software desired to be protected has to be responsible and last paragraph recites that "wherein access to said software desired to be protected is being provided without causing a said operation being performed", so the security module 16 as well as the information therein of Wiedemer (4,796,181) cannot meet identity means/software/information of claims 1, 12, 14 as amended because they are for enabling billing operation which being user responsible operation, to take place .

Although Wiedemer (5,155,680) also discloses a billing system and password protection, the password protection, as readable on col. 14, lines 4-7, is an "independent utility for providing secure data access and telecommunications capability for a personal computer even when pay-per-use billing is not desired". It has no psychological barrier and an authorised user may allow other unauthorised user to use his password as well as the protected software. Therefore, Wiedemer (5,155,680) is not applicable to claim 12 as amended.

Independent claims 7, 10 as amended recites the "authorising software for permitting use of the software desired to be protected", is being effectively under the control of the user thereof, this implies that the rightful user(s) can use the authorising software to access the protected software without any restriction such as payment.

Therefore Wiedemer(4,796,181) cannot meet claims 7, 10 as amended.

The present invention as defined by claim 7 allow unrestricted rightful use of protected software while offering protection against unauthorised use by requiring the authorising software be contained in the protection software with the identity software, and can not be copied therefrom individually.

Note that claims 7 further recites that the software desired to be protected being publicly distributed by a system against unauthorised use and at the last paragraph, "the improvement resides in said protection depends on no hardware specific to said user".

Claim 10 requires information capable of being used essentially, but not in a form to be so used, by the processing device, in enabling operation(s) for which the rightful user(s) of the software desired to be protected, has to be responsible ; exists in an authorising program/means and being accessible to the user the authorising program/means .

Independent claims 16, 18, 20 as well as dependent claim 3 of independent claim 12, recite "a first software" which **recognises a processing device, at the present of a psychological barrier** and "a second software" for **thereafter permitting use of software desired to be protected thereon**. This is another innovative feature of the present invention not being suggested or disclosed by the cited prior art reference, either considered individually or in combination.

Particularly, Claim 16 as amended recites using "a first software being supplied to rightful user(s), from a software distribution system, with confidential information of rightful user(s) of the software desired to be protected therein", as a "psychological barrier". Further, at the last paragraph, "said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; and said steps d) to h) is being performed without causing a said tranaction take place" .

Claims 16 as amended recites that first software will recognise a processing device **in response to** information obtained from a user thereof being consistent with that confidential information therein. The phrase "in response to" implies no other pre-condition(s) including payment, is necessary for the recognition of processing device.

Further, new dependent claim 17 of claim 16 clearly indicates "consistent with the confidential information" is the only condition.

Both new independent claims 18, 20 recites at the last paragraph that "the first software is specific to **a user**", this implies the protected software is confined to the use of that user only.

New claim 18, in particular, recites "identity information/means for accessing a remote electronic transaction system an account of that user" and requires the account being valid, as a "psychological barrier".

And, the first software of claim 18 recognises a processing device, at a cost from that user for the first time. It is clearly understood that the cost is for the use of the protected software on that recognised processing device by that user, because thereafter no further charge therefor, as readable on step h).

Independent claims 18 further recites, at the **present** of that psychological barrier, the same cost will not be re-charged for recognising another processing device, so as to allow the protected software to be used thereon.

Thus, a user who has paid for the protected software, can use the same on any processing device he desires or on the original processing device even after changes in software/hardware, without being re-charged, by using a psychological barrier to assure the software distribution system that the protected software will continue to be used by that user.

New independent claims 20 is similar to dependent claim 3 of independent claim 12 in that both for protection of software distributed through a communication network, see claim 3, last line. It is respectfully submitted that, it is a common practice to those with ordinary skill in the art to use "recognition of processing device" to prevent unauthorised use of network distributed software and re-recognition is of course not allowed.

Note that, claims 20 is similar to independent claims 1, 12, 14 , requires presence of identity information/means for "operation(s) for which a rightful user of the software desired to be protected has to be responsible", as a "psychological barrier". But it requires "without causing **any** operation(s) for which the rightful user has to be responsible, being performed". This implies that no re-charging.

stored in another location in each software product, and each of those another locations is different in different software products so that it would not be discovered and altered. And, each such software product, when executed, will automatically check the unencrypted identity stored therein against the decryption result of the encrypted one, if they are not consistent, the software product will fail to operate. The identity or encrypted identity of the rightful user being included into each of the software products by the central computer at the time when the central computer is to supply the same to the user computer. Further, to prevent the AS sub-program from mistakenly regarding a software product which stored in the computer and which being not supplied from the central computer, as a software product under its control, the central computer may further include information in a third predetermined location of each software product for indicating this fact, that is, the software product being supplied from the central computer, to the AS sub-program and each software product will not operate if when being executed, it finds that information therein being altered.

It should be noted that the above embodiments are given by way of example only, and it will be obvious to those skilled in the art that various changes and modifications may be made without departing from the spirit of the present invention.

What is claimed is :

1.(Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Authorising software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said authorising software being for, when executed, 1) permitting use of said software desired to be protected on said computer ; 2)]

determining [the existence of] if identity [software in a memory] means/information, is existing in a processing device [under control of said computer] ;

using a favourable result of said determination as a pre-condition for said processing device providing user access to said software desired to be protected ;

wherein said identity [software] means/information

[being for use on said computer to provide information of said rightful or authorised user ; said information]

being essentially used [in] by a control means of said processing device for

enabling operation(s) for which [said] rightful [or authorised user] user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

[and the existence of said identity software in a memory means under control of said computer is being determined without a said operation being performed by said remote computer]

[wherein use of said software desired to be protected on said computer will not be permitted if said identity software is determined as being not existing in a memory means under control of said computer .]

2. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

[Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1, wherein further comprising software, when being executed, for]

authenticating said identity [software] means/information ;

[and if the result of the authentication of said identity software is unfavourable,]

said identity [software] means/information will [further] be determined as existing [not existing in a memory means under control of said computer], if the result of said authentication is favourable and as not existing if otherwise .

3. (First time Amended) A method for protecting software from unauthorised use ,

[Authorising software, stored in a device or existing physically on a medium,]

as claimed in claim [1] 12, wherein said software desired to be protected being a first software used on said processing device for determining third information related to hardware and/or software of said processing device ;

wherein further comprising [authenticating] second software for , when being executed, authenticating the computer on which [it] said second software runs as being [a particular predetermined computer] said processing device, basing on at least a part of said third information;

[and if the authentication result of the computer on which it runs is unfavourable, said authorising software will not permit use of said software desired to be protected and will permit use of said software desired to be protected]

and access to a third software will be provided if said authentication result [of the computer] is favourable ;

wherein said third software being distributed through a communication network to said rightful user.

[and said identity software is determined as existing in a memory means under control of the computer on which said authorising software runs].

4. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1,]
wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s).

5. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1,]
wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

6. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 5,
[Authorising software, stored in a device or existing physically on a medium, as claimed in claim 5,]
wherein [further comprising] said processing device having an encrypted identity of its rightful user ; and if one of said protected programs stored in said computer has a valid user identity which being not consistent with the decryption result of said encrypted identity [in] of said [authorising software] processing device,

[said authorising software will not permit] use of said protected programs will not be permitted and will be permitted if otherwise .

7. (Second time Amended) Protection software for use on a [computer] processing device, to protect [purchased computer] software publicly distributed by a system against unauthorised use [by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof] ;

said protection software comprising :

identity software [for use on said computer to provide information of said rightful or authorised user ;]

[said information being esentially] essentially used on said processing device in enabling operation(s) for which [said] rightful [or authorised user] user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of the user thereof for, when executed, [permitting use of] providing user access to said software desired to be protected [, on said computer] ;

wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually; and

wherein the improvement resides in said protection depends on no hardware specific to said user(s) .

8. (First time Amended) Protection software [, stored in a device or existing physically on a medium,] as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s) .

9. (First time Amended) Protection software [, stored in a device or existing physically on a medium,] as claimed in claim 7, wherein said authorising software [includes] contains said identity software.

10. (Second time Amended) Authorising program/means [for use on a computer] used in a processing device, to protect other [computer] software against unauthorised use ; [by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof] ;

said authorising program/means being effectively under the control of the user thereof for, [when executed,] providing access to [permitting use of] said software desired to be protected [on said computer] ;

wherein information [of] related to [said] rightful [or authorised user] user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said information being capable of being used essentially, but not in a form to be so used , [used] by said processing device in enabling operation(s) for which said rightful [or authorised user] user(s) has to be responsible .

11. (First time Amended) Authorising program/means [, stored in a device or existing physically on a medium,] as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s).

12. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Protection software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said protection software comprising :]

obtaining a first information from a user of a processing device having an identity software/means ;

using said first information received being correct as a pre-condition for said processing device providing user access to said software desired to be protected;

wherein said identity software/means being for [, with password protection against used by unauthorised user,] providing a second information [of said] related to rightful [or authorised user] user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being essentially used by said processing device in enabling operation(s) for which said rightful [or authorised user] user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

[authorising software for, when executed, permitting use of said software desired to be protected on said computer ;]

[wherein use of said software desired to be protected will not be permitted if a correct password not entered by user .]

13. (First time Amended) A method for protecting software from unauthorised use , [Authorising program , stored in a device or existing physically on a medium,] as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s) and said first information being a password.

14. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Authorising software for use on a computer to protect other computer software by discouraging a rightful or authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said authorising software being for, when executed, 1) permitting use of said software desired to be protected on said computer ; 2)]

authenticating identity [software] information/means [existing in a memory means under control of said computer] associated with a control means of a processing device ;

using a favourable result of said authentication as a pre-condition for said control means providing user access to said software desired to be protected ;

wherein said identity [software being for use on said computer to provide information of said rightful or authorised user ;]

[said] information/means being essentially used by said control means for [in] enabling operation(s) for which [said] rightful [or authorised user] user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

[wherein use of said software desired to be protected will not be permitted if the result of said authentication of said identity software is not favourable .]

15. (First time Amended) A method for protecting software from unauthorised use , [Authorising program , stored in a device or existing physically on a medium,] as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful [or authorised user] user(s).

16. (First time Amended) A method for protecting software distributed by a system from unauthorised use , comprising the steps of :

a) obtaining by a processing means of said system, confidential information of rightful user(s) of said software desired to be protected ;

b) creating by said processing means, a first software with said confidential information therein ;

c) transferring from said system, said first software to a processing device under control of said rightful user(s) ;

d) thereafter, obtaining by said first software running on said processing device , first information from the user thereof ;

e) determining by said first software, from said processing device second information related to the hardware or/and software thereof for future reference in step f) below, in response to said first information obtained being consistent with said confidential information therein ;

f) thereafter, authenticating by a second software, the processing device onwhich said second software is being used, basing on at least a part of said second information ;

h) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

wherein said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; and said steps d) to h) is being performed without causing a said tranaction take place .

[Protection software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;

said protection software comprising :

identity software for, with protection against used by unauthorised user, providing information of said rightful or authorised user ;

said information being in enabling operation(s) for which said rightful or authorised user has to be responsible ;

authorising software for, when executed, permitting use of said software desired to be protected on said computer ;

wherein use of said software desired to be protected will not be permitted if said protected identity software is not being caused to be usable by correct information obtained from user .]

17. A method for protecting software distributed by a system from unauthorised use, as claimed by claim 16, wherein "said first information obtained being consistent with said confidential information" being the only condition for performing said determination in said step e).

18. A method for protecting software from unauthorised use, comprising the steps of :

a) transferring from a software distribution system, said software desired to be protected to a processing device under control of a user ;

b) transferring from said software distribution system, a first and second software to said processing device ;

c) determining by said first software running on said processing device, say first processing device, if identity information/means which being essentially used by a control means of said processing device for accessing in a remote electronic transaction system an account of said user, is present in said processing device ;

d) establishing a communication between said first software and a control means of said remote electronic transaction system, for verifying said account is a valid account, by said control means of said remote electronic transaction system to said first software ;

e) using by said first software, favourable results of said determination of presence and verification as pre-conditions for determining from said processing device information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said user by said software distribution system, for the first time said steps a) to e) being carried out ; thereafter

f) authenticating by said second software, the processing device onwhich said second software is being used, say, second processing device, basing on at least a part of said information related to said hardware or/and software ;

g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing device, with no charge ;

if the result of said determination of consistence is not favourable, repeat at least said steps c) to g) with said second processing device, without re-charging from said user said cost ;

wherein said first and second software being specific to said user.

19. A method for protecting software distributed by a system from unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to g) .

20. A method for protecting software distributed by a system through a communication network, from unauthorised use, comprising the steps of :

a) creating by said system, a first software ;

wherein "the presence of identity information/means which being essentially used by a control means of a processing device for enabling operation(s) for which a rightful user of said software desired to be protected has to be responsible, in said processing device" ; is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

b) transferring from said system, said first software to said processing device ;

c) determining by said first software running on said processing device meeting said precondition, first information related to the hardware or/and software of said processing device , for future reference in step e) below ;

d) thereafter, determining by a second software, from the processing device onwhich said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

repeat at least said steps c) to f) if said result of said determination of consistence is not favourable, without causing **any** operation(s) for which said rightful user has to be responsible, being performed ;

wherein said first and second software being specific to said rightful user.

another copy of #12

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant and Inventor	Ho Keung, TSE.
Title	
Filing Date	07/09/98
Application Number	09/112,276
Group Art Unit	2132
Examiner	Gilberto Barron Jr.
Postal Address	P.O. Box 54670, North Point Post Office, Hong Kong.
H.K. Tel & FAX	(852) 8105, 1090 (852) 8105, 1091
Email	t9224@netscape.net

By Airmail & Fax

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Sir,

Amendment Proposal Dated 7, May 2001

Pls change the title to read as "Protection of software from unauthorised use by means of a psychological barrier".

Pls amend claims 3, 16-20 by the replacement sheet submitted herewith.

Pls note that in claim 20, lines 1,2, the phrase "through a communication network" is being deleted, because it is not needed to preclude prior art related to selling software other than through a communication network, such as software stored in a disk as a commercial product etc, as claim 20 specifies "the presence of identity information/means as a precondition for recognising a processing device", which is a limitation already good enough for the purpose. Similarly, the last 2 lines of claim 3, "wherein said third software being distributed through a communication network to said rightful user" is also deleted.

Respectfully submitted,

Ho Keung, Tse.

2. A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/information ;

said identity means/information will be determined as existing , if the result of said authentication is favourable and as not existing if otherwise .

3. (second time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being [a] first software used on said processing device for determining third information related to hardware and/or software of said processing device ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing device, basing on at least a part of said third information;

and access to [a] third software will be provided if said authentication result is favourable .

[wherein said third software being distributed through a communication network to said rightful user]

15. A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

16. (Second time Amended) A method for protecting software distributed by a system from unauthorised use , comprising the steps of :

a) obtaining by a processing means of said system, confidential information of rightful user(s) of said software desired to be protected ;

b) creating by said processing means, [a] first software with said confidential information therein ;

c) transferring from said system, said first software to a processing device [under control of said rightful user(s)] ;

d) [thereafter,] obtaining by said first software running on said processing device , first information from the user thereof ;

e) determining by said first software, from said processing device second information related to the hardware or/and software thereof for future reference in step f) below, in response to said first information obtained being consistent with said confidential information therein ;

f) thereafter, authenticating by [a] second software, the processing device onwhich said second software is being used, basing on at least a part of said second information ;

h) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

wherein said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; and said steps d) to h) is being performed without causing a said tranaction take place .

17. (First time Amended) A method for protecting software [distributed by a system] from unauthorised use, as claimed by claim [16] 12, wherein ["said first information obtained being consistent with said confidential information" being the only condition for performing said determination in said step e)] said software desired to be protected being purchased commercial software.

18. (First time Amended) A method for protecting software from unauthorised use, comprising the steps of :

a) transferring from a software distribution system, said software desired to be protected to a processing device [under control of a user] ;

b) transferring from said software distribution system, [a] first and second software which being specific to a user, to said processing device ;

c) [determining by said first software running on said processing device, say first processing device, if identity information/means which being essentially used by a control means of said processing device for accessing in a remote electronic transaction system an account of said user, is present in said processing device ;]

[d)] establishing a communication between said first software running on said processing device, and a control means of [said] a remote electronic transaction system ;

d) [for] verifying said [account is] user having a valid account, by said control means of said remote electronic transaction system to said first software ;

e) using by said first software, a favourable [results] result of said [determination of presence and] verification as [pre-conditions] a pre-condition for determining from said processing device information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said user by said software distribution system, for [the first time] said steps a) to e) being carried out ; thereafter

f) authenticating by said second software, the processing device onwhich said second software is being used, say, second processing device, basing on at least a part of said information related to said hardware or/and software ;

g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing device, with no charge ;

if the result of said [determination of consistence] authentication is not favourable, repeat at least said steps c) to g) with said second processing device, without re-charging from said user said cost .

[wherein said first and second software being specific to said user.]

19. (First time Amended) A method for protecting software [distributed by a system] from unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to g) .

20. (First time Amended) A method for protecting software distributed by a system [through a communication network,] from unauthorised use, comprising the steps of :

a) creating by said system, [a] first software ;

wherein "the presence of identity information/means which being essentially used by a control means of a processing device for enabling operation(s) for which a rightful user of said software desired to be protected has to be responsible, in said processing device" ; is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

b) transferring from said system, said first software to said processing device ;

c) determining by said first software running on said processing device meeting said precondition, first information related to the hardware or/and software of said processing device , for future reference in step e) below ;

d) thereafter, determining by [a] second software, from the processing device onwhich said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

repeat at least said steps c) to f) if said result of said determination of consistence is not favourable, without causing any operation(s) for which said rightful user has to be responsible, being performed ;

wherein said first and second software being specific to said rightful user.